WHAT IS CLAIMED IS:

1

2

3

4

1 1. A computer-readable medium or propagated signal having embodied 2 thereon a computer program configured to determine whether a user is permitted to 3 access a business object when executing a software application of an enterprise information technology system, the medium or signal comprising one or more code 4 5 segments configured to: 6 use a permission object to determine whether a user associated with an entry in 7 user information is permitted to access a data object associated with a data object type, 8 wherein: 9 the entry in the user information associates the user with a user affiliation. 10 the permission object identifies: 11 a user affiliation to which the permission object applies, 12 a data object type to which the permission object applies such that the data 13 object type is associated with multiple attributes and each data object having the 14 data object type is associated with the multiple attributes. 15 a permission attribute identifying one of the multiple attributes, and 16 a permission value for the permission attribute, and 17 the user is permitted to access the data object when (1) the user affiliation that is associated with the user is the same user affiliation as the user affiliation to which the 18 19 permission object applies, (2) the data object type of the data object is the same data 20 object type as the data object type to which the permission object applies, and (3) a value 21 of an attribute of the multiple attributes associated with the data object is consistent with 22 the permission value of the permission attribute and the attribute corresponds to the 23 permission attribute.

2. The medium or signal of claim 1 wherein the one or more code segments are further configured to permit the user to access the data object when the value of the attribute of one of the multiple attributes associated with the data object is the same as the permission value of the permission attribute.

| 1 | 3. | The medium or signal of claim 1 wherein the one or more code segments |
|---|-----------------|---|
| 2 | are further co | nfigured to permit the user to access the data object when the value of the |
| 3 | attribute of or | ne of the multiple attributes associated with the data object is the within a |
| 4 | range specifie | ed by the permission value of the permission attribute. |

- 4. The medium or signal of claim 1 wherein the one or more code segments are further configured to permit the user to access the data object when the value of the attribute of one of the multiple attributes associated with the data object is one of enumerated values specified by the permission value of the permission attribute.
 - 5. The medium or signal of claim 1 wherein:

the permission object identifies an attribute group having one or more attributes of the multiple attributes associated with the data object type, and

the one or more code segments are further configured to permit the user to access an attribute of the data object only when the attribute of the data object corresponds to an attribute of the attribute group of the permission object.

6. The medium or signal of claim 5 wherein:

the permission object identifies a second attribute group having one or more attributes of the multiple attributes associated with the data object type, a second permission attribute identifying one of the multiple attributes, and a second permission value for the second permission attribute, associates the second permission attribute and the second permission value with the second attribute group, and associates the permission attribute and permission value with the attribute group, and

the one or more code segments are further configured to permit the user to access an attribute of the data object only when the attribute of the data object corresponds to an attribute of the second attribute group of the permission object and a value of an attribute of one of the multiple attributes associated with the data object is consistent with the second permission value of the second permission attribute.

7. The medium or signal of claim 1 wherein:

| 2 | the permission object identifies a permitted action, and |
|----|---|
| 3 | the one or more code segments are further configured to permit the user to access |
| 4 | the data object and perform an action on the data object when the action is consistent with |
| 5 | the permitted action identified in the permission object. |
| | \checkmark |
| 1 | 8. A method for determining whether a user is permitted to access a business |
| 2 | object when executing a software application of an enterprise information technology |
| 3 | system, the method comprising: |
| 4 | using a permission object to determine whether a user associated with an entry in |
| 5 | user information is permitted to access a data object associated with a data object type, |
| 6 | wherein: |
| 7 | the entry in the user information associates the user with a user affiliation, |
| 8 | the permission object identifies: |
| 9 | a user affiliation to which the permission object applies, |
| 10 | a data object type to which the permission object applies such that the data |
| 11 | object type is associated with multiple attributes and each data object having the |
| 12 | data object type is associated with the multiple attributes, |
| 13 | a permission attribute identifying one of the multiple attributes, and |
| 14 | a permission value for the permission attribute, and |
| 15 | the user is permitted to access the data object when (1) the user affiliation that is |
| 16 | associated with the user is the same user affiliation as the user affiliation to which the |
| 17 | permission object applies, (2) the data object type of the data object is the same data |
| 18 | object type as the data object type to which the permission object applies, and (3) a value |
| 19 | of an attribute of the multiple attributes associated with the data object is consistent with |
| 20 | the permission value of the permission attribute and the attribute corresponds to the |
| | |

9. The method of claim 8 further comprising permitting the user to access the data object when the value of the attribute of one of the multiple attributes associated with the data object is the same as the permission value of the permission attribute.

permission attribute.

| 1 | 10. The method of claim 8 further comprising permitting the user to access the |
|--|---|
| 2 | data object when the value of the attribute of one of the multiple attributes associated |
| 3 | with the data object is the within a range specified by the permission value of the |
| 4 | permission attribute. |
| | |
| 1 | 11. The method of claim 8 further comprising permitting the user to access the |
| 2 | data object when the value of the attribute of one of the multiple attributes associated |
| 3 | with the data object is one of enumerated values specified by the permission value of the |
| 4 | permission attribute. |
| | |
| 1 | 12. The method of claim 8 wherein the permission object identifies an |
| 2 | attribute group having one or more attributes of the multiple attributes associated with the |
| 3 | data object type, the method further comprising permitting the user to access an attribute |
| 4 | of the data object only when the attribute of the data object corresponds to an attribute of |
| 5 | the attribute group of the permission object. |
| | |
| | ? |
| 1 | 13. A computer system for determining whether a user is permitted to access a |
| 1 2 | · |
| | 13. A computer system for determining whether a user is permitted to access a |
| 2 | 13. A computer system for determining whether a user is permitted to access a data object when executing a software application of an enterprise information |
| 2 | 13. A computer system for determining whether a user is permitted to access a data object when executing a software application of an enterprise information technology system, the system comprising: |
| 2 3 4 | 13. A computer system for determining whether a user is permitted to access a data object when executing a software application of an enterprise information technology system, the system comprising: a data repository for access control information for software having data objects, each data object (1) being associated with a data object type having multiple attributes, |
| 2 3 4 5 | 13. A computer system for determining whether a user is permitted to access a data object when executing a software application of an enterprise information technology system, the system comprising: a data repository for access control information for software having data objects, |
| 2 3 4 5 6 | 13. A computer system for determining whether a user is permitted to access a data object when executing a software application of an enterprise information technology system, the system comprising: a data repository for access control information for software having data objects, each data object (1) being associated with a data object type having multiple attributes, (2) having multiple attributes that are the same as the multiple attributes of the data object |
| 2 3 4 5 6 7 | 13. A computer system for determining whether a user is permitted to access a data object when executing a software application of an enterprise information technology system, the system comprising: a data repository for access control information for software having data objects, each data object (1) being associated with a data object type having multiple attributes, (2) having multiple attributes that are the same as the multiple attributes of the data object type to which the data object is associated, and (3) having a value associated with each |
| 2 3 4 5 6 7 8 | 13. A computer system for determining whether a user is permitted to access a data object when executing a software application of an enterprise information technology system, the system comprising: a data repository for access control information for software having data objects, each data object (1) being associated with a data object type having multiple attributes, (2) having multiple attributes that are the same as the multiple attributes of the data object type to which the data object is associated, and (3) having a value associated with each attribute of the multiple attributes, the data repository including: |
| 2 3 4 5 6 7 8 | 13. A computer system for determining whether a user is permitted to access a data object when executing a software application of an enterprise information technology system, the system comprising: a data repository for access control information for software having data objects, each data object (1) being associated with a data object type having multiple attributes, (2) having multiple attributes that are the same as the multiple attributes of the data object type to which the data object is associated, and (3) having a value associated with each attribute of the multiple attributes, the data repository including: user information that associates a user affiliation with a user of the |
| 2 3 4 5 6 7 8 9 | data object when executing a software application of an enterprise information technology system, the system comprising: a data repository for access control information for software having data objects, each data object (1) being associated with a data object type having multiple attributes, (2) having multiple attributes that are the same as the multiple attributes of the data object type to which the data object is associated, and (3) having a value associated with each attribute of the multiple attributes, the data repository including: user information that associates a user affiliation with a user of the software application, and |
| 2 3 4 5 6 7 8 9 10 11 | 13. A computer system for determining whether a user is permitted to access a data object when executing a software application of an enterprise information technology system, the system comprising: a data repository for access control information for software having data objects, each data object (1) being associated with a data object type having multiple attributes, (2) having multiple attributes that are the same as the multiple attributes of the data object type to which the data object is associated, and (3) having a value associated with each attribute of the multiple attributes, the data repository including: user information that associates a user affiliation with a user of the software application, and permission information having multiple permission objects, each |

15

permission attribute; and

16 an executable software module that causes: 17 a comparison of a value of an attribute of the multiple attributes associated 18 with a data object to which a user seeks to access such that the attribute 19 corresponds to the permission attribute of a permission object with the permission 20 value of the permission object, and 21 an indication that a user is permitted to access a data object when the value 22 of the attribute associated with the data object is consistent with the permission 23 value of the permission object. 1 14. The system of claim 13 wherein the executable software module causes an 2 indication that a user is permitted to access the data object when the value of the attribute 3 of one of the multiple attributes associated with the data object is the same as the 4 permission value of the permission attribute. 1 15. The system of claim 13 wherein the executable software module causes an 2 indication that a user is permitted to access the data object when the value of the attribute 3 of one of the multiple attributes associated with the data object is the within a range 4 specified by the permission value of the permission attribute. 1 16. The system of claim 13 wherein the executable software module causes an 2 indication that a user is permitted to access the data object when the value of the attribute 3 of one of the multiple attributes associated with the data object is one of enumerated 4 values specified by the permission value of the permission attribute. 1 17. The system of claim 13 wherein: 2 the permission object identifies an attribute group having one or more attributes of the multiple attributes associated with the data object type, and 3 4 the executable software module causes an indication that a user is permitted to 5 access an attribute of the data object only when the attribute of the data object 6 corresponds to an attribute of the attribute group of the permission object.

18. The system of claim 17 wherein:

the permission object identifies a second attribute group having one or more attributes of the multiple attributes associated with the data object type, a second permission attribute identifying one of the multiple attributes, and a second permission value for the second permission attribute, associates the second permission attribute and the second permission value with the second attribute group, and associates the permission attribute and permission value with the attribute group, and the executable software module causes an indication that a user is permitted to access an attribute of the data object only when the attribute of the data object corresponds to an attribute of the second attribute group of the permission object and a value of an attribute of one of the multiple attributes associated with the data object is consistent with the second permission value of the second permission attribute.

- 19. The system of claim 13 wherein:
- 2 the permission object identifies a permitted action, and
- 3 the executable software module causes an indication that a user is permitted to
- 4 access the data object and perform an action on the data object when the action is
- 5 consistent with the permitted action identified in the permission object.